SSFN – a SCION ISD in Switzerland

Secure Swiss Finance Network SCION use case

Fritz Steinmann <Fritz.Steinmann@six-group.com>

06/11/2023

SIX – Who we are

SIX operates the Swiss Financial Infrastructure:

- Swiss Stock Exchange (Listing & Trading)
- Financial Information (Reference & Market Data, Indices)
- Securities Services (Central Security Depository, Central Counterparty, Clearing & Settlement)
- Banking Services (Billing & Payment Services, Debit & Mobile Services, ATM Services)

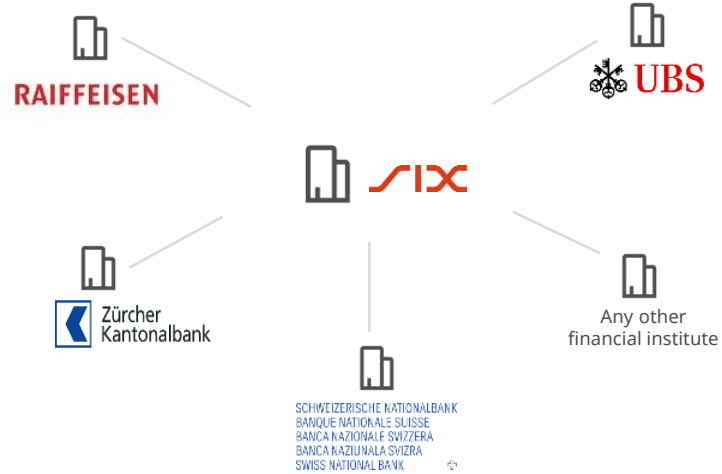
- Interbank services are provided by a private network operated by commercial telco providers
- SIX maintains connections to other banks pan-Europe and in other markets globally

Business and Technical Requirements for a new Interbank Network

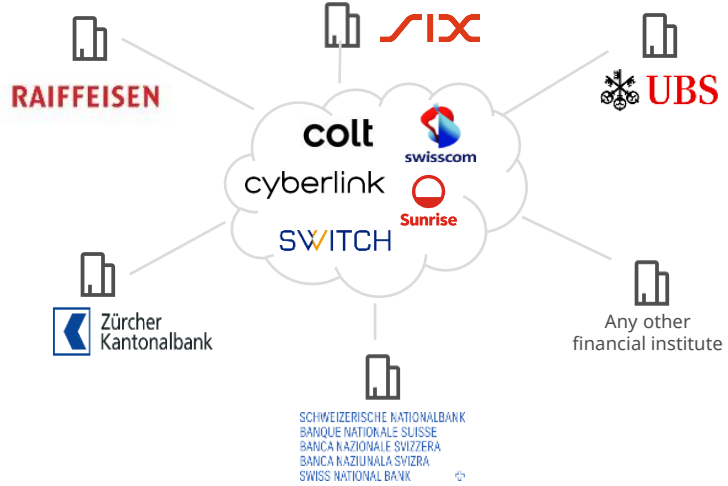
- Trends and Challenges
  - Real-Time systems such as the Swiss payments system and other critical infrastructures form the strong core for the financial system and must have strongest possible protection
  - Increasing reliance on public networks – the Internet – for communications between financial institutions, bank branches and infrastructures
  - Vulnerability of data in transport is a risk (e.g., due to denial of service or man in the middle attacks)
  - Current solutions to address risks are inflexible and costly
- Requirements for a new Interbank Network
  - A secure and resilient communication network for payments and other critical infrastructures
  - Protection against cyber risks: enforceable governance and boundaries
  - Trust in the network – know the location / path of data in transit
  - Flexible communication between participants: any-to-any architecture instead of (virtual) point-to-point connections
  - Delivered by the financial community and telecom providers – no change in business model

SSFN – A Secure and Resilient Communication Network for Interbank traffic

Today
Centralized «Hub and Spoke» architecture



Vision
Community-based, «any-to-any», Internet-like architecture



Why SCION?

- Before starting, a thorough analysis was started
  - Comparison between different new Internet technologies was done
  - Alternatively, replacing MPLS by another MPLS network was considered
  - SD-WAN was briefly discussed, but is not suited for a multi-provider, multi-product, multi-customer market
- SCION promised to meet the requirements
- SCION had already achieved a high level of maturity in productive use (Swiss National Bank, Swiss Government)
- There was already a close collaboration between SIX and ETH, where SCION was originally researched and developed

What is different in using SCION compared to other technologies?

- SCION allows for local, user-centric, enforceable governance
- Governance can be split from actual operations; the governance parties don’t need to be identical to those who operate the network
- ISD concept allows for complete isolation of trust
- Multiple operations models can be implemented, it allows for various business models

The Governance of SSFN Defines the Rules & Regulations of SSFN – Service Providers Must Qualify

Basic characteristic of SSFN

Regulated interaction between users and service providers (with rules defined by the governance and influenceable by users and service providers), but decentralized like the Internet.

Governance SSFN

Run/Use SSFN

Voting members SSFN (SIX, SNB, SWITCH)	SSFN Service provider [1] (Anapaya, service providers SIX, Sunrise, Swisscom, SWITCH, SIX)	SSFN User (SIX customers)
Responsible for SSFNs rules and a functioning Trust Root Configuration (TRC)	Providing the necessary services for the data exchange based on the SCION protocol and the SSFN rulebook	Purchase of services from approved SSFN service providers
How to Be Part of SSFN?	Is accepted as service provider for SSFN, following a transparent onboarding process and contractually confirming to continuously adhere to requirements criteria	Is qualified by using an eligible service from a SIX entity (e.g. SIC) offered via SSFN

1| Service providers can also offer SCION-related services for other ISDs

TRC Creation and Maintenance

- From research perspective, TRC creation and life cycle is well established and well documented (see SCION Control-Plane PKI draft RFC , https://datatracker.ietf.org/doc/draft-dekater-scion-pki/)
- In practice, key and TRC creation ceremonies must be designed according to ISD requirements
- In a multi-party governed ISD virtual TRC ceremonies have proved to be effective and viable
- Elements in the TRC:
  - ISD ID
  - Purpose
  - Core and authoritative participants (ASes)
  - Validity period
  - Voting Quorum
  - Certificates (CA root, regular and sensitive voting)
  - Some other parameters

TRC Creation and Maintenance

ISD ID

Purpose / Description

Voting Quorum

Core and authoritative participants (ASes)

Certificates (CA root, regular and sensitive voting)

Validity period

```
anapaya@trc-hoster: /opt/trc-ceremony-20231026
isd                 = 70
description         = """ISD 70 bildet die Grundlage für SSFN, das Secure Swiss Finance Network.

Kurzbeschreibung des SSFN ISD

1. SSFN ist ein Kommunikationsservice für den Schweizer Finanzplatz.
2. SSFN ermöglicht einen vom Internet getrennten Austausch von Daten unter den Nutzern, jedoch mit I
3. Die SSFN-Governance (Voting Member) regelt, welche Partei SSFN nutzen (z.B. Bank) bzw. Dienstleis
4. Die Datenübermittlung wird von verschiedenen Carriern erbracht, mit von den Carriern definierten
5. SSFN ist unabhängig von der Anwendung bzw. Applikation, welche SSFN nutzt und bietet keine Versch

Die Regeln des SSFN sind im SSFN Reglement festgehalten und sind von allen SSFN Teilnehmern (Nutzer,
serial_version      = 3
base_version        = 1
voting_quorum       = 2
votes               = [1, 3, 6]
core_ases           = ["559", "3303", "6730"]
authoritative_ases  = ["559", "3303", "6730"]
cert_files          = [
        "snb/sensitive-voting.crt",
        "snb/regular-voting.crt",
        "six/sensitive-voting.crt",
        "six/regular-voting.crt",
        "six/cp-root.crt",
        "switch/sensitive-voting.crt",
        "switch/regular-voting.crt",
        "switch/cp-root.crt",
]
no_trust_reset      = false
grace_period        = "15d"

[validity]
not_before = 1700006400 # 2023-11-15 00:00:00 UTC
validity   = "395d"
```

TRC Creation and Maintenance

- The process is basically to:
  - Collect and verify required material (CA root certificates, Sensitive and Regular Voting Certificates)
  - Agree on required parameters (as indicated above)
  - Generate payload (object container)
  - Sign by authoritative parties, verify signatures and content
  - Combine signatures and create final TRC container

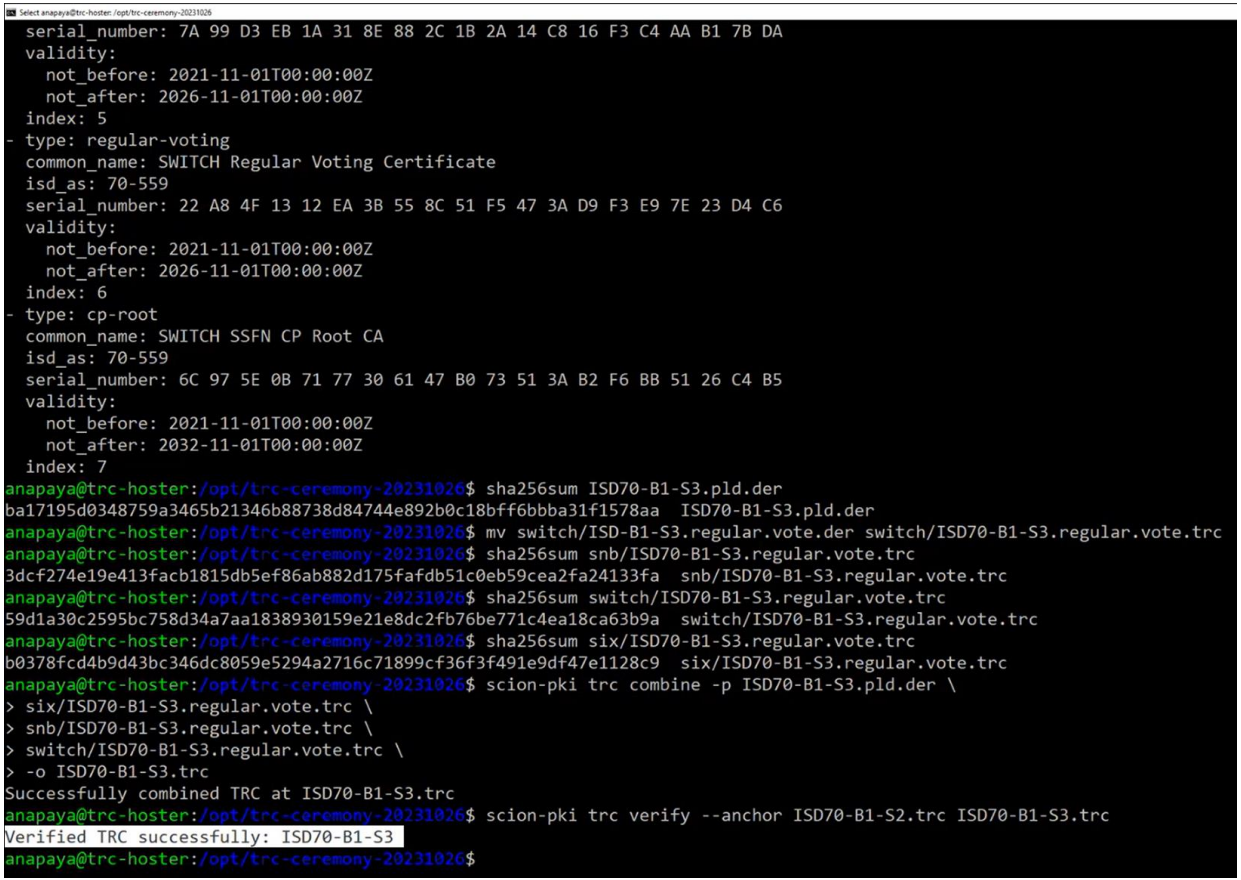
```
anapaya@trc-hoster:/opt/trc-ceremony-20231026$ scion-pki trc payload --predecessor ISD70-B1-S2.trc --out ISD70-B1-S3.pld.der --template ISD70-B1-S3.toml
Generating payload for TRC update.

required signatures:
- type: vote
  common name: SIX Regular Voting Certificate
  serial number: 37 F4 66 80 3D 1F E3 6F 77 CE 4C 42 73 D1 56 C3 0F DA D1 CD
- type: vote
  common name: SNB Regular Voting Certificate
  serial number: 37 92 22 59 3F 56 9E 78 3B A9 4A 63 9A 76 FA DC 01 1A 40 8E
- type: vote
  common name: SWITCH Regular Voting Certificate
  serial number: 22 A8 4F 13 12 EA 3B 55 8C 51 F5 47 3A D9 F3 E9 7E 23 D4 C6

Successfully created payload at ISD70-B1-S3.pld.der
anapaya@trc-hoster:/opt/trc-ceremony-20231026$
```

TRC Creation and Maintenance

- SSFN ISD TRC has been first created in November 2021
- Validity period was set to 395 days
- It was renewed successfully in 2022 and 2023
- Dissemination in the SSFN ISD is seamless



Challenges / How could IETF help?

- Lack of adoption
  - Although SSFN is a completely functional and flawlessly operating network, it is but a lighthouse implementation
  - None of the bigger network software companies picked up SCION implementation so far
  - None of the bigger ISP’s showing interest in deploying SCION so far
- Lack of operational authorities (e.g., numbering) / global governance → addressed by SCION Association
- Lack of standardization → can be addressed at IETF
- There will be more work at IETF needed
  - Continuing work on Internet drafts towards RFC’s
  - Aligning with other work
  - Exploring more options